

Business risks from naive use of RFID in tracking, tracing and logistics

Lothar Fritsch, Norwegian Computing Center, Oslo, Norway. E-Mail: Lothar.Fritsch@NR.no

Abstract

Logistics, food tracing, tracking of deliveries and customs processing expect large gains in efficiency from the use of RFID. Brand manufacturers hope for the effective detection of brand forgery and smuggling along the logistics chain. Large trial projects for shelf maintenance and customer self-service are under way in supermarket chains. The vision of the “Internet of things” aims at a logistics chain reaching from the producer’s meadow into the consumer’s refrigerator, providing optimized logistics, security, tracing, and health functionality.

However, the naïve application of such technologies can create hazards that need to be considered, and managed in the planning process and throughout the whole application lifecycle. This article shifts the focus from RFID tags and readers to the long-term implications of the complete tracking system, and discusses ways of discovering and preventing risks.

1 Introduction

A public debate has occurred concerning the new risks for personal data. However, businesses face severe risks from naïve application of RFID and tracing schemes as well. This article will present and classify the risks and provide guidance for risk-mitigating construction of RFID in logistics, tracing and tracking.

1.1 The popular view on RFID risks

RFIDs are presented as “Spychips” [1] in the popular press, supported by various grassroots privacy movements. The press has a preference on tracking, tracing, and related privacy invasions, visible in debates on RFID passports, driver’s licenses, e-tickets and consumer articles with RFID.

NGOs are forming wherever a major player introduces RFID to a consumer value chain, gaining considerable press exposure, e.g. in case of the Metro Future Store project.

RFID is often perceived insecure and immature (e.g. with frequent reporting of hacked transportation tickets such as the Oyster card, and “cloned” RFID ID-cards. The Elvis-Presley-Passport-RFID that was accepted by airline check-in machines is still a popular video on YouTube¹. Discussions about people tracking, remote reading of shopping bags, and passport RFID security problems have led to products sold on popular web stores such as the “RFID Blocking Wallet” and the “Pointprotect ePass RFID Silver Ghost” protection envelope for passports².

A general theme in the public discussion is the asymmetry of benefits and risks. It is generally perceived that introducers of RFID automation gain the efficiency benefits, while consumers will be exposed to risks. Consumers worry about such risks. There are risks for the introducers as well, as explained in the next sections.

1.2 EPC, tags and personal data

Public worries about privacy implications fueled debate about data protection and privacy regulation. Here, the facts are confusing on a first sight. Proponents of RFID technology claim that there are no privacy problems, as RFID is only used to track objects. The GS1-EPCglobal – the major RFID promoting organization – published “Guidelines on Electronic Product Codes (EPC) for Consumer Products” [2]. These explain that “The Electronic Product Code does not contain, collect or store any personally identifiable information,” which is not what will give confidence to a worried consumer. EPCglobal suggests education measures to “in appropriate ways (...) familiarize consumers with the EPC logo and to help consumers understand the technology and its benefits.” Consumers shall be informed about choices to remove tags from products.

However, in the European Union as well as overseas, data protection specialists agree that a RFID system does collect personal data as soon as the tag is person-relatable. Some “dark scenarios” have been compiled in the SWAMI project [3]. Such personal data association can happen on the fly, for a truck driver and the freight on the lorry, the mail delivery person and his mail cart, or a consumer walking the roads with RFID e-tickets, e-passports and shopping bags or boxes with tags. The implications have been illustrated in a book on profiling in the FIDIS project [4]. Based on this observation, the Privacy Commissioner of Ontario in Canada published privacy guidelines for RFID use³. Focus should be on the whole system, and privacy shall be considered from start. Consent from participants in RFID based applications shall be collected. The 2008 EU’s draft recommendations⁴ fully integrate RFID

¹ <http://www.youtube.com/watch?v=4HngStyEm4s>, as of 16.Apr. 2009

² <http://www.pointprotect.de/>, as of 16.Apr. 2009

³ http://www.ipc.on.ca/images/Resources/up-2006_06_19rfid.pdf, as of 17.Apr. 2009

⁴ http://ec.europa.eu/information_society/eeurope/i2010/docs/high_level_group/draft_recommendation_rfid.pdf, as of 17.Apr. 2009

applications with the data protection framework, and even suggest that risk analysis and audits could be required in the near future:

1. RFID operators shall conduct privacy risk assessment!
2. Risk assessments should honor stakes, and cover all stakeholders!
3. Take appropriate technical and organizational measures to mitigate the privacy risks!
4. Assign a responsible person for audit and adaptation of the above!
5. Privacy & security risk management shall be aligned.
6. The privacy risk assessment summary must be published latest upon deployment of the RFID application.

A third example of possible business impact and unexpected cost in RFID deployment is the Norwegian passport that contains a RFID-readable biometric authentication chip. The data protection authority has required from the police authority that supervises the passports:

1. Politidirektoratet shall assess privacy risks of biometric passport handling with respect to §13 personopplysningsloven (POL) og §2-4 personopplysningsforskriften.
2. Politidirektoratet shall provide all necessary information to applicants and holders of biometric passports acc. to §19 POL.
3. Politidirektoratet must design and implement an internal privacy controlling system according to §14 POL. The system must not be outsourced.

These tasks are not exactly core competences of a police organization, and therefore create serious staff and equipment expenses for the RFID system owner – the government. This section's conclusion is that data protection regulation can impose serious cost on RFID system owners and operators if it is cared for too late.

1.3 Business implications of asymmetric risks

Asymmetric risks could fire back on a business when they become endemic in society. In particular, systems spreading asymmetric risks could face:

1. Regulation of established infrastructures involving increased change cost, management cost and training expenses;
2. Compliance and non-compliance cost, such as audits, fines, exclusion from tender and legal cost;
3. Reputation damage, resulting in customer loss, competitive loss, branding damage and lost business.

An example of asymmetric risks is the treatment of information privacy. Many internet-based businesses establish very simple authentication and protection measures, while their users might have to go through extraordinary efforts to fight damages later, e.g. after a data breach or a stolen password have been abused. This is called the “duality of privacy risks” by Fritsch and Abie in [5]. Privacy protec-

tion is an ICT management issue. It causes cost-of-ownership, no matter whether a sophisticated privacy concept is implemented, or not. In 2004, the Ponemon Institute conducted a study for IBM [6]. It provides a cost factor model and provides some insight into corporate spending patterns for privacy management in large corporations. The authors define a “total privacy cost framework”. The approach is to compare the cost of non-compliance to privacy requirements to the cost of investing in privacy management with respect to its effect. The assumption is that the optimum in privacy spending is where the expenditure equals the non-compliance cost. This results in the calculation of privacy protection cost not with the goal of maximum privacy, but cheapest compliance.

From this, some significant insight can be gained. The survey lists the privacy costs ranked by direct cost. IT systems (e.g. PET or IDM), are on the third position of the most expensive cost factors, amounting about one-third of the cost of privacy office, and less than 50% of the cost for training. Beyond PET, there eight other cost factors exist that are policy-intense or involve specialized employees, e.g. lawyers. As a conclusion, privacy technology by itself is not a main cost driver – policies, enforcement, legal counsel and many other factors outnumber the cost of PET used. In a recent study, the European Network Security Agency (ENISA) found principal vulnerabilities to be considered with NFC applications [7].

Concluding this section, the major lesson learned is that asymmetric risks might cause large cost on the owner of an RFID infrastructure later in time, while the possibly risky effects can backfire upon the infrastructure and harm the business.

2 RFID in application contexts

RFID technology is deployed into application contexts. Many of the possible risks can only be modeled and observed in consideration of the application context.

Much research has been published on RFID tag security, reader protocols, and access control to the tag's data fields. However, the privacy and business intelligence risks are created by a link between tags and a particular context, such as a person, a product, a vendor or a location. Thus, both the middleware and the application context are critical inputs to risk analysis. Unfortunately, most technical descriptions describe tag & reader products detached from the application context. For this reason, the next section presents a multi-layered model of RFID applications that covers the whole system.

2.1 A layered model of RFID applications

With the introduction of NFC technology, readers became mobile, while NFC phones playing the role of “active tags” provide the tags with vast processing and communications power. For our paper, we will use the scenario model below.

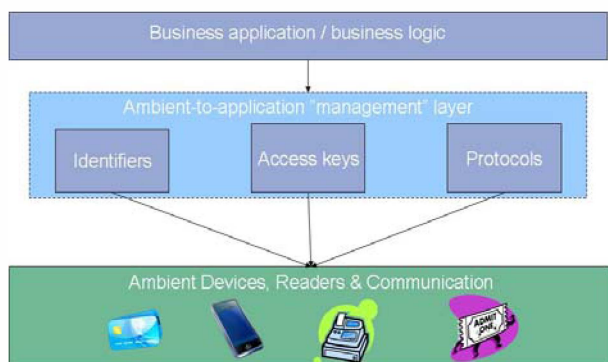


Figure 1: RFID in context – scenario assumption.

We divide the integrated world of RFID application into the three layers shown in fig.1:

1. Business application layer: This layer executes the application logic.
2. Ambient middleware layer: this layer connects the application world to the ambient world of tags, readers and NFC devices, and manages its specific aspects such as key handling, tag management and tracking.
3. Ambient device layer: Here, the tags, their protocols, the readers and interacting devices are found.

Security requirements and threats are different for each layer, and the establishment of trust requires different perspectives on the RFID security threats to businesses.

2.2 Trust and security issues in RFID applications

Divided into the three layers, the security issues are illustrated in fig. 2. On the ambient device layer, we identify issues mainly related to access control, authentication and protected storage. The middleware layer has issues with distance-bounding, malicious components, communications protocols security and eavesdropping. The application layer involves tracking & tracing, identifier handling, identity management, possible revocation and key management issues on a higher level.

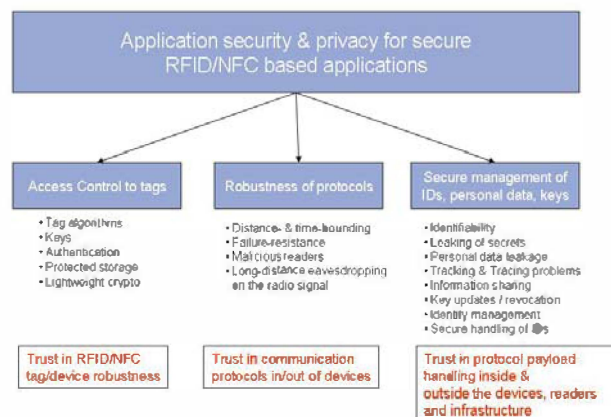


Figure 2: RFID security issues by layer.

3 Business risks– Example Cases

This section will discuss risks posed by RFID use based on the layer model presented in section 2, and provide guidance on risk handling.

3.1 Case 1: The Boycott Phone

Many proponents of RFID-based food tracing stress the transparency created by such a system. Consumers shall feel much safer when they can use a mobile phone to “scan” a product label or RFID tag. They would receive information about the food production, the farmer, and the processing. In Norway, Nortura’s demonstrator goes as far as showing the animal’s trail on a green meadow⁵ on mobile phones. However, imagine this direct access in the hands of a typical, global non-government pressure group or a ruthless marketer. Can you imagine a “boycott phone” (see Figure 3), which has a program installed that tells the consumer which articles to leave behind in the supermarket. Or worse, maybe a competing market that is telling the phone owner which of the articles are cheaper elsewhere? Such secondary use of its RFID tags are not on the agenda of today’s retail market chains – but their RFID supply chain could easily support them on their own expenses.



Figure 3: The "Boycott phone" exploits consumer product RFID labels that were intended for food tracing and food safety.

3.2 Case 2: Retail Espionage

Retail detail information is worth money. Information about the sale of a particular product, its popularity in a certain area, or with certain social groups is important market and competition information. This need is the very reason for the existence of market intelligence corporations such as AC Nielsen. Today, they depend upon voluntary data exchange with retail chains, mystery shopping, and consumer interviews. However, RFID will surely come to their attention once the market density of both logistics and

⁵ Nortura’s demonstrator was developed in the food research program of the Norwegian Research Council, see <http://spor.nortura.no>, as of 21.Apr. 2009

consumer RFID tags is high enough. From data gathering at factory exit gates or transport hubs such as Padborg on the Danish-German border up to walking through competitors super markets with a “scanner backpack” or parking a vehicle with scanning equipment right in front of the market’s exit door, the possibilities are many. For 3rd parties hungry for business intelligence, such methods can even use statistical methods to bypass scanner technology shortages, e.g. in concurrent channels and signal outreach. Serious business information is at stake when RFID is deployed naively in this scenario.

3.3 Case 3: Information leakage

Food tracing applications have caught the attention of the RFID industry and the computer industry since governments consider regulation of food safety procedures in the European Union and elsewhere. Food tracing from the farm to the consumer refrigerator is supposed to enable fast recalls of bad food, and provide authorities and producers to trace the source of the problem swiftly. Middleware vendors such as IBM advertise platforms that will maintain tracing data and related RFID tags. Many visions foresee the consumer with mobile phones, checking on the cow’s first name while shopping at the meat counter. Such a picturesque vision of full production chain transparency can seriously backfire on the production stakeholders when the information is made transparent in ignorance of the real “food scandal” procedures. Imagine a “bad fish found in supermarket” warning as shown in Figure 4.

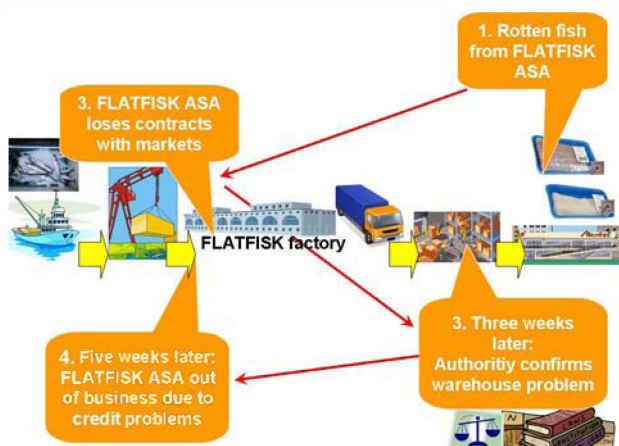


Figure 4: Production chain information leakage can be a serious threat to businesses.

Here, a certain amount of time passes before the authorities are done gathering tracing information, samples, and lab test results, and concluding the cause of the food problem. In our example, cooling in a warehouse didn’t work. However, the consumer and the media caught up “FLATFISK ASA” from the RFID tags, and get their name into the newspapers. In consequence, the factory loses business, and faces severe problems on the market. It might very well go bankrupt before the real cause was found. In any case, the businesses’ name will be stigmatized until a considerable amount of marketing budget has been spent. How many small farms, family-owned food processors or, e.g., small Norwegian fish producers can afford a few

months of lost business, and a multi-million image campaign? They might feel that they are forced into a RFID-based tracing scheme that will not benefit, but threaten their business if it is not designed well, according to all stakeholders’ information security and privacy needs.

3.4 Some far-fetched surprises

Imagine a world where...

- A vendor’s trash (packages, products) will be tracked around the globe, even 20 years after production, until it turns up on a polluted site in Africa – and on some NGO’s agenda;
- The city trash removal facilities read RFIDs on package waste to bill the producers for the trash processed;
- Corporate tax & toll is adjusted based on scanners at borders, ware houses and waste dumps.

These far-fetched RFID applications might easily emerge in a decade or two, as a consequence of RFID mass use. They can backfire the consumers’ RFID privacy problem on the businesses. In this context, the recommendation from data protection offices on detachable tags, tag deactivation and ID encryption might look useful for businesses. However, EPCglobal is just about to introduce unique, TID identifiers to EPC compatible tags⁶, which leaves the deactivation to the implementation of both the tag KILL command and the middleware that accesses the tags [8].

4 Risk management and mitigation

This section introduces risk analysis and risk mitigation based both on processes and technology. The section on risk modeling analyzes possible information leakage problems concerning RFID tags, and the ISO 27000 information security management system’s risk management approach for information security

4.1 Risk analysis and risk management

Risk analysis and risk impact analysis are standard procedures in many professions. For information system security risks, recently a number of standards for non-technical security management procedures have evolved – the ISO 27000 family. Unlike earlier standards, such as ISO 15408 (Common Criteria), the early ISO 17799 and ISO 27000 focus on management procedures of information security. The reason is the changing environment, with expiring technology, new threats, and ageing computing equipment. Security and privacy problems can arise surprisingly at some time in the future. ISO 27000 suggest a cycle of plan-do-check-act (PDCA) for information security management. It begins with assessments and planning of risk

⁶ According to a statement by Florian Michahelles and Mikko Lehtonen made in the RFIDJournal on Sep. 22, 2008, the introduction of unique TID would prevent tag counterfeits. See <http://www.rfidjournal.com/article/view/4332>, as of 20.Apr..2009

mitigation procedures, and installs responsibilities and procedures for information security management in an organization. Frequent analysis of events, re-assessment of risks and adjustment of the risk mitigation measures are performed as a persistent, regular activity. Some market segments, e.g. the financial sector, are required by law to implement similar procedures. In some cases, data protection authorities prescribe such management approaches, as presented above in section 1.3.

Risk assessment creates a risk of all important “information assets” (computers, data bases, processes, documents, etc.) that are critical to the organization. For each of the assets, a risk analysis based on possible risks, and impacts of risk events are compiled. Next, risks are prioritized, and for each of them, risk mitigation strategies for impact minimization are designed. Risk mitigation involves technical, procedural and managerial work. Risk assessment, mitigation strategies and the resulting design requirements for both technology and procedures need to be documented, and in consequence, staff trained to apply them. On management level, there must be a control group called “information security management system forum” that reacts to crises and adjusts risk mitigation strategies.

ISO 27000 was clearly designed for systems that are, e.g. under the control of a single organization. RFID systems, however, are clusters of readers, middleware, tags and applications that are only connected through standard interfaces, seldom belong to one organization. A privacy risk impact assessment for an EPC-compatible RFID infrastructure should involve hundreds of parties, and in addition all stakeholders that are not related to the RFID-using organizations, but who might get involved with tagged objects. This is a major challenge, where even the mid-term impact assessment is very hard.

As a starting point, each stakeholder on a RFID application should perform risk analysis based on all stakeholder's stakes – not only his own. Section 4.2 will summarize some of these views in checklist questions.

4.2 “Identity theft” and RFID threats

Tags tell stories. Standards like the EPC are designed to manage stories associated with tags. By using radio transmission as the access medium, these stories can be captured “on air”. In this article, the focus is on recognizable identifiers such as tag numbers, EPC's TID codes, and other data that is stored accessibly on tags. This article is not concerned with cryptographic attacks on tag security mechanisms, but many of the insights below hold for data gathered from broken tags or decrypted reader-tag communications. The analysis below assumes that we observe tags that contain an easily readable data field, such as a TID, an EPC code or some serial number. In the simplest RFID application model, such an identifier is used to correlate a tagged object with a database record.

Tag identifiers are binary byte strings stored in the tag's memory. Typically, these numbers are:

- random numbers
- sequential numbers introduced by the tag vendor

- 'serial' numbers associated with object vendor's objects
- static numbers used as identifiers
- specific patterns, e.g. following some standard such as EPC or bar codes, or a vendor's internal codification.

In addition to the tag identifier, much of a tag's context can easily be inferred by capture of some obvious information, such as:

- object-related context (such as product type, and vendor)
- time data (when does a tag turn up, how often, in what sequences?)
- location (where does a tag show up?)
- correlation (what other tags are correlated in time or space? Are there sequence patterns over time?)

Tags can be observed to establish a number of relationships to other tags, depending on how they are observed together, or in various contexts.

- Tag ownership : One tag 'owns' other tags that, thereby building a hierarchy. This could be the case e.g. for a RFID-tagged container filled with other tagged objects.
- Mobility : Tags can be static or dynamic in time and space.
- Crowding : Tags can turn up in correlated crowds of tags, which is observable through common mobility or static ownership relationships.
- Lifecycle : Tags can follow a particular 'lifecycle' pattern, revealing their context, type or use, and thereby establishing the membership in a 'class' of tags.

Threats posed by static tags

Summarizing the above, static tags are exposed to three major information leakage threats:

1. Re-identification of a tag based on a former observation;
2. Linkability of a tag to either
 - another tag;
 - context information such as time, space, a person;
3. Crowd-correlation of a tag in a crowd of other tags.
4. Correlation of tags with specific contexts
5. Correlation of tags with sequences, e.g. time and location.

Risk mitigation

Risk mitigation strategies are composed of technical and organizational measures. Below, a checklist for identifier risks and countermeasures is presented. It contains questions for the areas of privacy, business intelligence, tag identifiers, and tag robustness. The list should be used to analyze the own organizations vulnerabilities, and in addition it can be used to communicate with middleware and

application system vendors. The last mentioned parties should be able to explain identifier management, database access and correlation risks, and risk mitigation strategies.

Checklist for RFID identifier risks

RFID identifier risk check list
► Are you aware of all contextual information that can be correlated to your tags? ▪ delivery frequency & destinations ▪ return quotas & retail rates ▪ predictable identifiers (e.g. serial number sequences) ► Countermeasures: ▪ Identifier management ▪ Encryption from tag to application level ▪ Use tags without individual numbers
► Do your tags contain interpretable information? ▪ product keys ▪ receivers or customer information ▪ indications of object value ▪ origin information ► Countermeasures: ▪ Identifier management ▪ Encryption & Access control ▪ Tag self-destruct / deactivation or self-sealing
► Are your tags person-relatable? ▪ Equipment check-out ▪ e-tickets ▪ consumer items ▪ ID cards, door cards, passports, bank cards ► Countermeasures ▪ De-activation (including chip serial number!) ▪ Identity management ▪ Privacy risk assessment & audits ▪ Privacy-enhancing technology (PET)
► Are your tags securely bound to the tagged objects? ▪ Tag-switching destroys food tracing ROI (e.g. rotten meat with "good" tag) ▪ Fraudulent customers switch product tags to shop cheaper ► Countermeasures ▪ Redundant information on tag & object ▪ "Biometrics" derived from the object stored on tag ▪ Fingerprinting techniques based on secrets

4 Summary

Long-term information leakage is a risk in RFID projects. The risk might not be obvious until the outreach of the applications has grown large. Deployment of RFID projects should consider the whole application chain, not only the tags and readers. Much business intelligence and many regulatory compliance problems can occur. Projects should be aware of them early. The two major areas of concern should be identifier management and access control.

Identifier management

Who owns the tag identifiers, and the data base related to the tags, and how will it be protected from unauthorized use? The tag is out of the security perimeter of the vendor and often out of the using organizations as well.

The use of anonymizing schemes, cryptographic methods, randomized numbering schemes and zero-knowledge-protocols for identifier management should be considered. Such technology has been under research, for example in the PRIME project [9] and the FIDIS Network of Excellence [10]. Identifiers should always be analyzed for information leakage and possible risks before they are deployed.

Access control & Information flow

Multi-level and role-based access control models are used in server & mainframe computing for more than three decades. Many of these security models implemented on a "need to know" basis, where only the necessary information is accessible to each stakeholder..

But today's RFID approaches aim for maximum transparency, efficient data access, and global standardization. Information flow analysis and access control models are essential to protect business secrets, and should be a part of RFID application systems as well.

5 References

- [1] C. Albrecht and L. McIntyre, *Spychips: How Major Corporations and Government Plan to Track Your Every Purchase and Watch Your Every Move*. Plume, 2006.
- [2] EPCglobal, *EPCglobal Guidelines on EPC for Consumer Products*. 2005.
- [3] L. Maghiros, Y. Punie, S. Delaitre, P. Hert, S. Gutwirth, W. Schreurs, A. Moscibroda, M. Friedewald, R. Linden, D. Wright, E. Vildjiounaite and P. Alahuhta, "Safeguards in a world of ambient intelligence," in *Intelligent Environments*, vol. 2, Athens: IEEE Computer Society, 2006,.
- [4] L. Fritsch, "Profiling and Location-Based Services," in *Profiling the European Citizen - Cross-Disciplinary Perspectives*, M. Hildebrandt and S. Gutwirth, Ed. Dordrecht: Springer Netherlands, 2008, pp. 147-160.
- [5] L. Fritsch and H. Abie, "A Road Map to the Management of Privacy Risks in Information Systems," in *Konferenzband Sicherheit 2008, Lecture Notes in Informatics LNI 128*, vol. 128, Gesellschaft f. Informatik (GI), Ed. Bonn: Gesellschaft für Informatik, 2008, pp. 1-15.
- [6] Ponemon Institute, *The Cost of Privacy Study*. Tucson, Arizona: 2004.
- [7] I. Naumann (eds.), G. Hogben (eds.), L. Fritsch and et. al., *Security issues in the context of authentication using mobile devices (Mobile eID)*. Heraklion, Greece: 2008.
- [8] GS1, *Specification for the RFID Air Interface*. 2005.

- [9] PRIME, Privacy and Identity Management for Europe. 2003.
- [10] FIDIS, FIDIS Deliverable D13.1: Identity and impact of privacy-enhancing technology. 2007.

Acknowledgements

The work that led to this article was funded by the Norwegian Research Council's basic research funding and through RISKnet – the Norwegian and Nordic Network on Information Security and Societal Risks. I thank Bjarte M. Østvold for the many hours of discussions, planning and brainstorming.